PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 12/58, 29/06, 12/22 — A1

(11) International Publication Number: WO 00/31931

(43) International Publication Date: 2 June 2000 (02.06.00)

(21) International Application Number: PCT/SE99/02021

(22) International Filing Date: 8 November 1999 (08.11.99)

(30) Priority Data:
09/198,822 24 November 1998 (24.11.98) US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

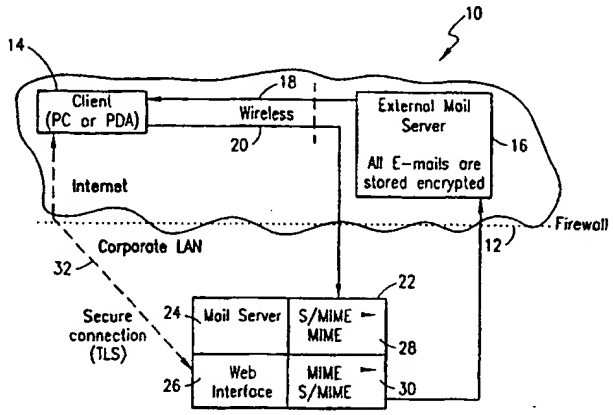
(72) Inventor: GEHRMANN, Christian; Backvägen 38, S-126 47 Hägersten (SE).

(74) Agent: ERICSSON RADIO SYSTEMS AB; Patent Support/Ericsson Research, S-164 80 Stockholm (SE).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND SYSTEM FOR SECURING DATA OBJECTS



(57) Abstract

A method and system are disclosed for securing primarily private e-mail that can be conveyed to and from a user via an open network such as the Internet. Essentially, the e-mail messages are encrypted with a secure digital envelope type protocol which can be based on the use of digital certificates. An example of such a digital envelope encryption protocol is the S/MIME protocol. As such, a domain-to-user security relationship is used instead of a user-to-user or domain-to-domain security relationship. For example, a mobile radiotelephone user of a corporate network (22) can have certain incoming e-mail forwarded to an external mail server (16) (e.g., in the Internet). The mail to be forwarded is first encrypted into a secure digital envelope format (e.g.,-S/MIME format) with the user's secret key. Consequently, the protected e-mail from the corporate network (22) can be forwarded to the user via the external mail server (16) (e.g., in the Internet) without compromising security.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND SYSTEM FOR SECURING DATA OBJECTS

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention relates generally to the telecommunications field and, in particular, to a method and system for securing data objects such as electronic mail (e-mail).

Description of Related Art

Mobile radiotelephone users have a significant problem gaining access to corporate information when they are on travel or at home. Today, most remote access solutions for gaining access to corporate information for such mobile users are based on the use of dial-up connections to dedicated modem pools. Another solution for obtaining the desired corporate information is to route the information to or from the user using an arbitrary Internet connection and an encrypted "tunnel" to a gateway at the border between the Internet and the corporate Local Area Network (LAN). However, the problem with such a solution is that the user's equipment is located outside the corporate network, and consequently, that equipment can be quite vulnerable to security attacks and breaches.

It is expected that, in the near future, numerous high-speed Internet connections will become available. Consequently, it is currently desirable to design solutions for gaining access to corporate network information that will work for any Internet Protocol (IP) connection. In particular, it is currently desirable to provide a secure and flexible solution for a specific type of corporate information service: e-mail.

There are numerous ways to provide secure access to corporate information over an IP connection. As such, different protocols for providing secure access to such information have been, or are being, standardized by the Internet Engineering Task Force (IETF). The security protection can be placed at a number of different levels in the communications stack. However, there are essentially two basic

protection approaches that can be used: application protection and transport protection. The Secure Multi-purpose Internet Mail Extension (S/MIME) Standard currently being developed in the IETF is an example of an application protection approach, while the Transport Layer Security (TLS), SSH, and Internet Protocol Security (IPSEC) protocols are for transport protection.

Low level information protection can be beneficial because the services can be provided without requiring any changes to the applications involved. On the other hand, low level protection protocols (e.g., IPSEC protocol) require substantial modifications to the operating systems involved. Furthermore, information that is protected only during transport requires additional protection when the information is ultimately stored at the clients' locations and servers.

In that regard, the S/MIME Standard should be able to provide adequate protection for e-mail messages while they are stored at a user's terminal and/or mail server. For example, the S/MIME protection approach should make it possible to provide e-mail services that are totally open at the Internet and extremely easy to access. As such, it is expected that this model of open but protected information will be one of the more important security models in the future.

The standard Netscape® and Microsoft® e-mail tools support the S/MIME protocol. As such, the S/MIME Standard should provide a way to encrypt MIME information in a way that is flexible and secure. The S/MIME standard will be a combination of public key encryption and symmetric encryption. The symmetric key encryption will be used to encrypt the actual information content in the MIME messages, and the public keys will be used to encrypt the symmetric key used for encryption of the MIME content, or for digitally signing the MIME message. The S/MIME approach will use digital certificates to check the validity of the public keys used.

Secure e-mail approaches such as S/MIME, are based on a point-to-point communication model. In other words, an arbitrary user in a network communicates with another user in the network, and the communication between the two users is secure. Unfortunately, however, such a point-to-point security

model does not fit well in a conventional corporate network architecture. Typically, a corporate network (e.g., LAN) is an IP-based private network, and its only access to the Internet is through a firewall. Consequently, it is intentionally made difficult to access information in the corporate network from the other side of the firewall. Furthermore, many users of the corporate network are not interested in maintaining encryption key information, or to have to look up such key information every time an e-mail message is to be sent to another user in the network. Simply put, it is a relatively difficult problem to implement a point-to-point security model for protecting e-mail in such large organizations as corporations. However, as described in detail below, the present invention successfully resolves the above-described problems.

SUMMARY OF THE INVENTION

In accordance with the present invention, a method and system are provided for securing private e-mail that can be conveyed to and from a user via an open network such as the Internet. Essentially, the e-mail messages are encrypted with a secure digital envelope type protocol which can be based on the use of digital certificates. An example of such a digital envelope encryption protocol is the S/MIME protocol. As such, a domain-to-user security relationship is used instead of a user-to-user or domain-to-domain security relationship. For example, in a preferred embodiment of the present invention, a mobile radiotelephone user of a corporate network can have certain incoming e-mail forwarded to an external mail server (e.g., in the Internet). The mail to be forwarded is first encrypted into a secure digital envelope format (e.g.,S/MIME format) with the user's secret key. Consequently, the protected e-mail from the corporate network can be forwarded to the user via the external mail server (e.g., in the Internet) without compromising security.

An important technical advantage of the present invention is that a mobile user can receive and view secure e-mail via an open network such as the Internet.

Another important technical advantage of the present invention is that a corporate network user's e-mail can be secured with a maximum of two digital

certificates required to obtain such protection.

Still another important technical advantage of the present invention is that the security of a user's e-mail is independent of the mail server used.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the method and apparatus of the present invention may be had by reference to the following detailed description when taken in conjunction with the accompanying drawings wherein:

FIGURE 1 is a diagram that illustrates a secure e-mail system and method that can be implemented in accordance with a preferred embodiment of the present invention; and

FIGURE 2 is a flow diagram of a method that can be used for encryption and decryption of e-mail using the S/MIME standard in accordance with the preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

The preferred embodiment of the present invention and its advantages are best understood by referring to FIGUREs 1-2 of the drawings, like numerals being used for like and corresponding parts of the various drawings. Essentially, in accordance with the present invention, a method and system are provided for securing private e-mail that can be conveyed to and from a user via an open network such as the Internet. The e-mail messages are encrypted with a secure digital envelope type protocol which can be based on the use of digital certificates. An example of such a digital envelope encryption protocol is the S/MIME protocol. As such, a domain-to-user security relationship is used instead of a user-to-user or domain-to-domain security relationship. For example, in a preferred embodiment of the present invention, a mobile radiotelephone user of a corporate network can have certain incoming e-mail forwarded to an external mail server (e.g., in the Internet). The mail to be forwarded is first encrypted into a secure digital envelope format (e.g.,S/MIME format) with the user's secret key. Consequently, the protected e-mail from the corporate network can be forwarded to the user via the external mail server (e.g., in the Internet) without

compromising security. As such, although the present invention is described herein primarily with respect to the protection of e-mail, the present invention can also apply to the protection of any data object, such as, for example, data programs, JAVA programs, or mobile code.

Specifically, FIGURE 1 is a diagram that illustrates a secure e-mail system and method that can be implemented in accordance with a preferred embodiment of the present invention. For this embodiment, an exemplary system 10 includes an open or public-access network (e.g., the Internet) and a private network (e.g., a corporate intranet or LAN). The two networks are typically separated by a firewall 12, which functions primarily to protect and maintain the confidentiality of the information stored in the private network.

The open network includes a mail server 16 (external to the private network). A user (e.g., user of the private network) can access the mail server 16 to receive and view e-mail with a personal computer (PC) or Personal Digital Assistant (PDA) 14. For this exemplary embodiment, the user is preferably a mobile radiotelephone user who can gain access to the mail server 16 over a conventional wireless connection 18. For example, the user's PC (or PDA) 14 can include a speech/data connection to a mobile radiotelephone, such as, for example, a cellular phone. The user's PC (or PDA) 14 can utilize a conventional e-mail application such as Netscape® mail or Microsoft Outlook Express® to forward or receive e-mail to or from the mail server 16 via the connection 18. Nevertheless, although a wireless connection 18 is shown, the scope of the present invention is not intended to be so limited, and can include the use of, for example, a wireline connection, fiber optic connection, etc. However, the use of a wireless connection 18 via a mobile phone is more convenient for a user who is periodically on the move (e.g., in an automobile, train, aircraft, etc.).

For this embodiment, the user's PC (or PDA) 14 is also connected to the corporate network (generally denoted as 22) via a wireless (or any other appropriate) connection 20. For example, the user's PC (or PDA) 14 can transfer data via a cellular phone over the wireless connection 20 to a dial-up modem at the corporate network 22. Additionally, the user's PC 14 can be connected to the corporate network's World-Wide Web (WWW) interface 26 via a secure connection 32 (e.g., using the

TLS protocol). The primary purpose for this secure connection 32 in the context of FIGURE 1 is to enable the user to formulate and convey an e-mail forwarding policy to the corporate network 22.

For this exemplary embodiment, the corporate network 22 includes a mail server 24 (e.g., on a corporate LAN). The Web interface 26 can be a conventional Web interface typically used for, among other things, maintaining e-mail forwarding policies responsive to users' directions. The corporate network 22 also includes a decryption unit 28 for decrypting an incoming e-mail message that has been encrypted using a packet or digital envelope cryptographic protocol (e.g., S/MIME). In this embodiment, the decryption unit 28 preferably includes a software application that can decrypt a secure digital envelope-formatted (e.g., S/MIME-protected) e-mail message conveyed via the connection 20 from the user's PC 14. An encryption unit 30 preferably includes a software application that functions to encrypt an outgoing e-mail message with a secure digital envelope format (e.g., from a MIME format to S/MIME format). The encrypted e-mail messages are coupled from the corporate network 22 to the external mail server 16 via a conventional data connection 34. For example, the corporate network 22 can be connected to an Internet mail server (16) via a Public Switched Telephone Network (PSTN) T1 line (34).

In operation (referring to the exemplary embodiment illustrated in FIGURE 1), a mobile phone user employs the PC (or PDA) 14 to send a message including e-mail forwarding policy instructions to the Web interface 26. Preferably, the e-mail forwarding policy message is transported via a secure connection 32 (e.g., using TLS, IPSEC or any other appropriate secure transport protocol) to the Web interface 26. This mail forwarding policy predetermines which e-mail messages are to be transported from the corporate network 22, and to what address (e.g., to the external mail server 16). For example, the user's e-mail forwarding policy can include instructions to forward all incoming e-mail messages from the corporate LAN to the external mail server, or just to forward certain e-mail messages only (e.g., just those arriving from a specific set of addresses, or having a certain priority). As such, the user's e-mail forwarding policy actually selected can be a matter of personal (or corporate) choice.

At this point, it is useful to describe in general how a secure digital envelope format can be used to implement the present invention. A secure digital envelope is a message, or information string, packed into a certain format to provide confidentiality, and/or integrity, and/or non-repudiation. In order to transform any clear-text message into a protected digital envelope format, a combination of symmetric and asymmetric cryptographic functions can be used. Unlike most secure data transport protocols, a digital envelope can be used for off-line decryption and integrity-checking. Once transformed into a secure cryptographic envelope format, a secure message can be decrypted and checked at any time by anyone who possesses a correct secret key. As mentioned earlier, the S/MIME standard is an example of a secure digital envelope format.

As an exemplary type of secure digital envelope format that can be used to implement the present invention, the S/MIME standard can provide confidentiality and/or integrity and non-repudiation protection for MIME messages. Encrypting a MIME message with a secret symmetric key provides confidentiality for the message, while using a digital signature provides integrity and non-repudiation for the message. In accordance with the S/MIME standard, a message can just be encrypted, just signed, or both encrypted and signed. The following description illustrates an exemplary method that can be used with the S/MIME standard to provide confidentiality, integrity and non-repudiation protection for a MIME message to be sent from one user to another.

For example, assume that a user, A, wants to send a MIME message, M, to an arbitrary user, B, using the S/MIME standard. Let "g" represent a public key encryption algorithm used for encryption so that for a public key pair, K_public and K_secret, an arbitrary message, L, will be encrypted as, L'=g(K_public,L), and decrypted as, L=g'(K_secret,L'). Let "e" represent a public key algorithm used for signing so that for a public key pair, K_public and K_secret, a short message, L, will be signed as S=e(K_secret,L). Let S'=e'(K_public,S). As such, an arbitrary signature, S, for the message, L, is valid if and only if S'=S. Let "h" represent a one-way hash function so that for any message, M, the function h(M) equals a 128 bit value, and that given M and h(M), it is computationally infeasible to find any other message, M', such

that h(M')=h(M). Given these exemplary conditions, a method that can be used for encryption and decryption using the S/MIME standard in accordance with the preferred embodiment of the present invention, is shown in FIGURE 2.

Referring to the assumptions and conditions described above and the exemplary method 200 shown in FIGURE 2, at step 201, user A (e.g., A's terminal) searches for a public encryption key, K_publicB, for user B. For example, such a key can be contained in a digital certificate signed by a trusted third party. At step 202, user A generates a random value for a key, K_s. At step 203, user A encrypts the message, M, using the key, K_s, and a symmetric encryption algorithm f, as C=f(K_s,M). At step 104, user A encrypts the key, K_s as K'=g(K_publicB,K_s). At step 105, user A holds the public key pair, K_publicA,K_secretA, to be used for signing messages. User A then computes a digital hash for the cipher text C, as C'=h(C), and uses the key, K_secretA, to sign C'as, S=e(K_secretA,C')=e(K_secretA,h(C)).

At step 206, user A (e.g., A's terminal) sends the message, (K',S,C), to user B together with a digital certificate (e.g., signed by a trusted third party) which contains the key, K_publicA. At step 207, user B (e.g., B's terminal) receives the message, (K',S,C), together with a certificate which contains the public key, K_publicA. At step 208, user B checks the signature of the certificate with the key, K_publicA. At step 209, if user B determines that the signature is correct, user B accepts the key, K_publicA, as the public signing key of user A. Otherwise, if the signature is incorrect, then user B considers the message (K',S,C) as invalid and can disregard the communication.

At step 210, user B calculates S'=e'(K_publicA,h(C)). At step 211, if user B determines that S'=S, then user B accepts the message (K'S,C) as a valid message from A. Otherwise, user B considers the message as invalid. At step 212, user B calculates K_s=(K_secretB,K'). At step 213, user B decrypts C as M=f'(K_s,C), and thus obtains the message, M, originally from user A.

Returning to FIGURE 1, and in the context of the preferred embodiment of the present invention, the e-mail to be forwarded (in accordance with the user's predetermined mail forwarding policy) from the corporate network (LAN) 22 to the

external network's (Internet) mail server 16 is first encrypted. For example, in this exemplary embodiment, the e-mail messages stored in the corporate network's mail server 24 are maintained in the MIME format. As such, using the exemplary method 200 described above, the encryption unit 30 can encrypt each e-mail message to be forwarded to the external mail server into an S/MIME format. If the user is employing a PDA (14) instead of a PC, the encryption unit 30 can encrypt the e-mail to be forwarded into the S/MIME format using symmetric keys shared between the network mail server 24 and the user's PDA 14. A digital certificate can be used to assure the integrity and non-repudiation of the message.

The S/MIME encrypted e-mail messages are transmitted from the network 22 to the external mail server 16 via the conventional connection 34. The encrypted e-mail is then maintained in the user's mailbox at the external mail server, until the user requests the mail for delivery to the PC (or PDA) 14. Using a conventional mail tool (e.g., Netscape mail or Microsoft's Outlook Express), the user's PC (or PDA) 14 can retrieve the encrypted mail from the external mail server 16 via the connection 18. Using the exemplary method 200 described above, the user's PC 14 can check the signature of the certificate and decrypt the mail from the S/MIME format to the MIME format. If a PDA (14) is used, it decrypts the received mail.

The mobile user can also transmit encrypted e-mail messages from the PC (or PDA) 14 to the network 22. For this embodiment, using the same method 200, the user's PC (or PDA) 14 encrypts the e-mail to be forwarded to the network 22 from the MIME format to an S/MIME format. mail server 22. The encrypted e-mail message (and a digital certificate associated with the mail server 22) is transmitted from the PC 14 to the decryption unit 28 via connection 20. The decryption unit 28 checks the digital certificate and then decrypts the received e-mail message from the S/MIME format to the MIME format. Notably, as opposed to the S/MIME approaches now under consideration, the present invention requires the use of only two digital certificates for authentication: the user's certificate for encrypted mail forwarded to the external mail server; and the corporate mail server's certificate for encrypted mail forwarded to the corporate network's mail server. A conventional Certificate Management System can be used in the corporate network's mail server 24 to handle

both the issuance of digital certificates and the publication of the revocation of such certificates, if so required.

In accordance with a second embodiment of the present invention, one or more e-mail mailing lists can be implemented and secured. For example, mailing lists currently are useful for large groups of people having some common interests in communicating by e-mail. In order to subscribe to a mailing list, a person can send certain subscription e-mail containing the e-mail messages intended for communication to a mailing list e-mail server. The subscription e-mail can contain the e-mail address where the subscriber desires to receive e-mail from the mailing list. All mail received by the mailing list server is forwarded to all mail addresses of subscribers to the list. At present, anyone who wishes to subscribe to an e-mail list may do so. As such, the only identity related to a subscriber is that subscriber's e-mail address. However, a problem is that e-mail address could be an anonymous address. In other words, it is currently not possible for a mailing list administrator to prevent malicious use of the list by certain subscribers. Moreover, all e-mail messages currently being sent to and from mailing list servers are sent in clear text. However, the secure e-mail gateway provided by the present invention can be used to prevent such problems.

For example, in accordance with the preferred embodiment of the present invention, the MIME to S/MIME (or S/MIME to MIME) e-mail gateway (e.g., units 24-30) can be used as a mailing list server. By requiring that all subscription messages be sent in S/MIME, for example, and be signed with a valid signature and certificate, the identity of the subscriber can be determined before allowing the subscriber to enter the mailing list in the server. By requiring that all messages sent to the mailing list server be encrypted with the gateway's key and signed by the user, the confidentiality and integrity of the mail received by the gateway 22 can be ensured. Before forwarding mail, the gateway 22 can encrypt the e-mail by using the receiver's certificate. Consequently, all messages sent to and from the mailing list (server) will be protected.

A preferred embodiment of the method and apparatus of the present invention has been illustrated in the accompanying Drawings and described in the foregoing

Detailed Description, it will be understood that the invention is not limited to the embodiment disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.

WHAT IS CLAIMED IS:

1. A system for protecting a data object to be delivered to a user of a private network via an open network, comprising:

a first server associated with said private network;

an encryption unit coupled to said first server, for encrypting said data object intended for said user; and

a second server associated with said open network, said second server coupled to said encryption unit and said first server, said second server including means for delivering said encrypted data object to said user.

2. The system of Claim 1, wherein said data object comprises an e-mail message.

3. The system of Claim 1, wherein said first server comprises a first mail server.

4. The system of Claim 3, wherein said second server comprises a second mail server.

5. The system of Claim 1, wherein said private network comprises a corporate LAN.

6. The system of Claim 1, wherein said open network comprises the Internet.

7. The system of Claim 1, wherein said encryption unit includes means for encrypting said data object to an S/MIME format.

8. The system of Claim 7, wherein said data object is encrypted with a secret symmetric key associated with said user.

9. The system of Claim 1, wherein said encryption unit includes means for encrypting said data object using a packet or digital envelope cryptographic protocol.

10. The system of Claim 1, further comprising:

a decryption unit coupled to said first server, for decrypting a data object received from said user.

11. The system of Claim 10, wherein said data object comprises an e-mail message.

12. The system of Claim 11, wherein said decryption unit includes means for decrypting said e-mail message from an S/MIME format to a MIME format.

13. The system of Claim 11, wherein said e-mail message is decrypted using a secret key associated with said first mail server.

14. The system of Claim 1, further comprising means for formulating a policy for forwarding an e-mail message from said first server to said second server.

15. The system of Claim 1, wherein said first server comprises a mailing list server.

16. A method for protecting a data object to be delivered to a user of a private network via an open network, comprising the steps of:

in said private network, encrypting said data object with a secret key associated with said user;

in accordance with a predetermined forwarding policy, forwarding said encrypted data object to a server in said open network;

said server delivering said encrypted data object to said user; and

decrypting said encrypted data object using said secret key.

17. The method of Claim 16, wherein said data object comprises an e-mail message.

18. The method of Claim 16, wherein said server comprises a mail server.

19. The method of Claim 16, wherein said private network comprises a corporate LAN.

20. The method of Claim 16, wherein said open network comprises the Internet.

21. The method of Claim 16, wherein said encrypting step comprises encrypting said data object to an S/MIME format.

22. The method of Claim 16, wherein said encrypting step comprises encrypting said data object using a packet or digital envelope cryptographic protocol.

23. The method of Claim 16, further comprising the step of decrypting a data object received from said user.

24. The method of Claim 23, wherein said data object comprises an e-mail message.

25. The method of Claim 24, wherein said decrypting step comprises decrypting said e-mail message from an S/MIME format to a MIME format.

26. The method of Claim 25, wherein said decrypting step comprises decrypting said e-mail message with a secret key associated with a mail server in said private network.

27. The method of Claim 16, further comprising the step of formulating a

policy for forwarding said data object from a first mail server in said private network to a second mail server in said open network.

28. The method of Claim 16, wherein said private network comprises a mailing list server.

29. A system for providing secure access to a data object intended for a user of a private network via an open network, said system comprising:

a gateway associated with said private network, said gateway configured to forward said data object intended for said user in accordance with a forwarding policy of said user;

an encryption unit coupled to said gateway for encrypting said data object to be forwarded; and

an external server associated with said open network for storing said encrypted data object forwarded from said private network, said external server enabling access to said encrypted data object by said user via said open network.

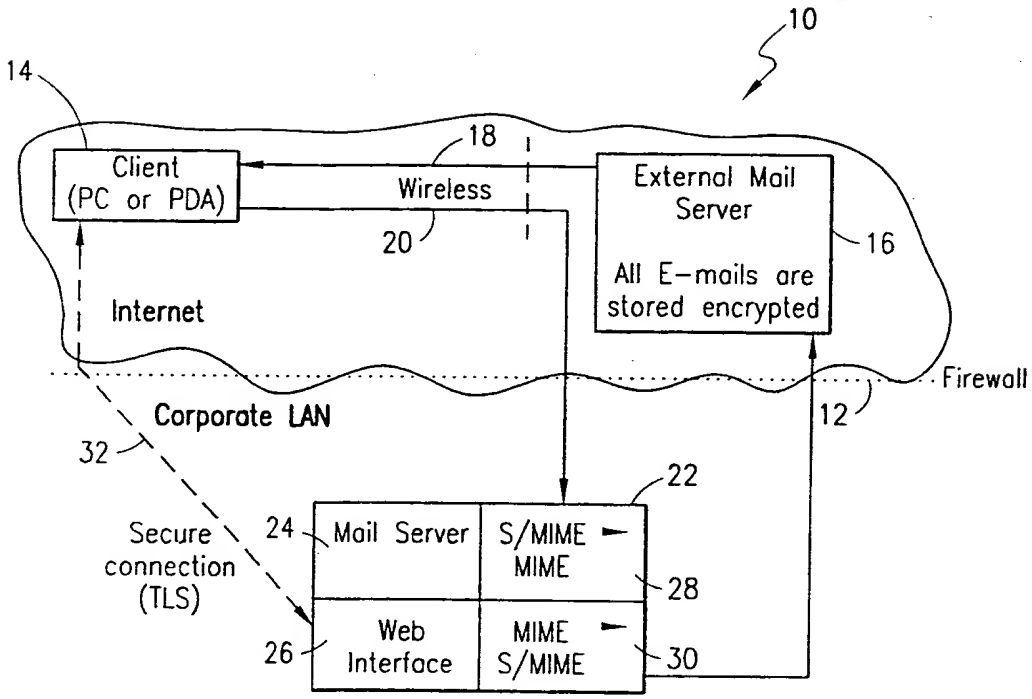

10
14
18
Client
(PC or PDA)
Wireless
External Mail
Server
16
20
All E-mails are
stored encrypted
Internet
Firewall
Corporate LAN
12
32
22
Secure
connection
(TLS)
24
Mail Server
S/MIME
MIME
28
Web
Interface
26
MIME
S/MIME
30

FIG. 1

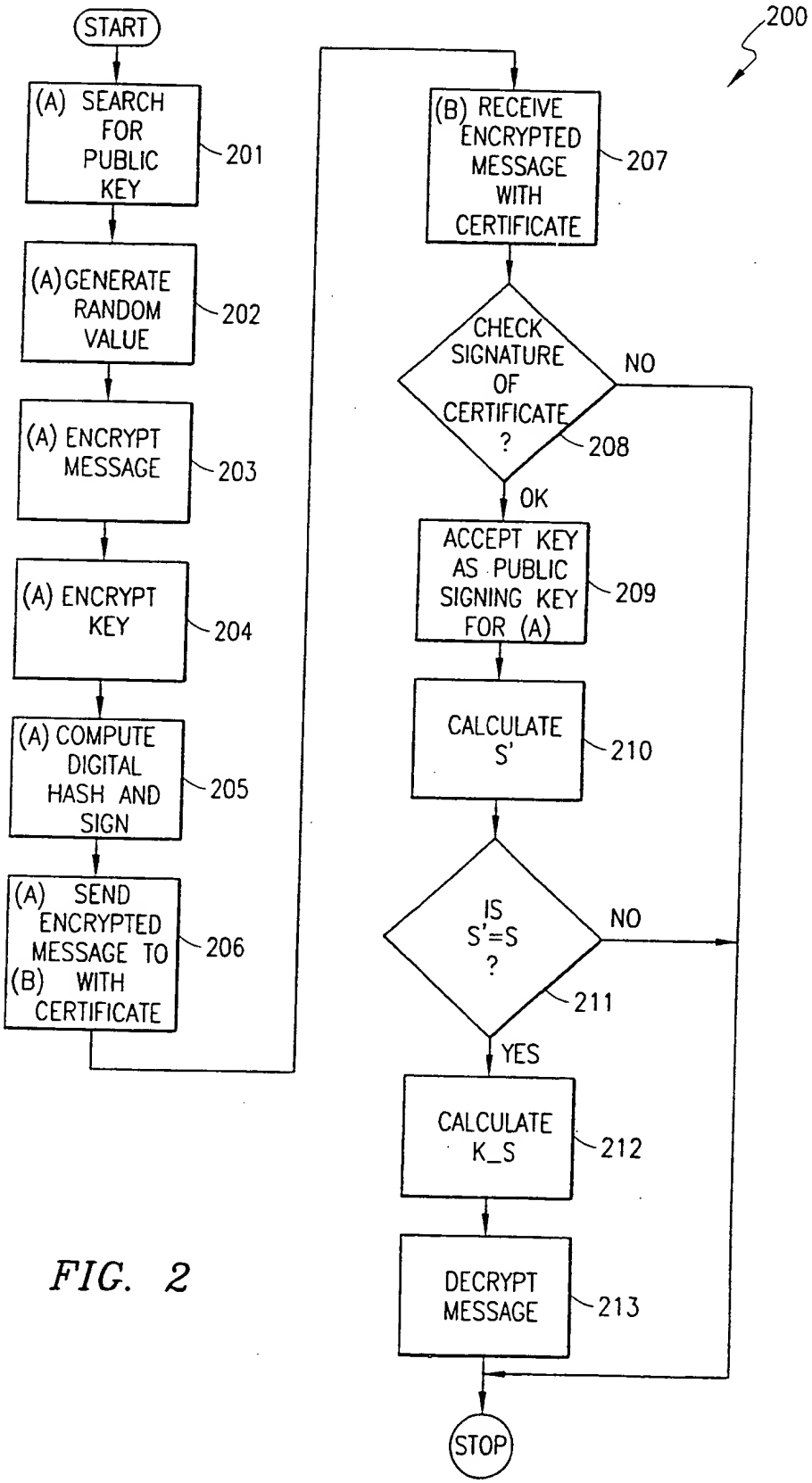


FIG. 2

INTERNATIONAL SEARCH REPORT

ernational Application No
PCT/SE 99/02021

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/58 H04L29/06 H04L12/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passagee	Relevant to claim No.
X	WO 97 47106 A (WEBTV NETWORKS INC) 11 December 1997 (1997-12-11) page 4, line 1 -page 5, line 4 page 9, line 10 -page 10, line 10 page 13, line 14 -page 17, line 18	1-3,6, 9-11,13, 16-18, 20,22-24
Y		5,7,8, 12,19, 21,25, 26,29

—

-/—

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 March 2000	23/03/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Poggio, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

ernational Application No
PCT/SE 99/02021

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 96 13113 A (SECURE COMPUTING CORP) 2 May 1996 (1996-05-02) abstract page 9, line 15 -page 11, line 15 page 14, line 1 - line 28 page 24, line 3 - line 24 figures 3,4,12	5,19,29
Y	LEVIEN R: "PROTECTING INTERNET E-MAIL FROM PRYING EYES" DATA COMMUNICATIONS, vol. 25, no. 6, 1 May 1996 (1996-05-01), page 117/118, 120, 122 XP000587586 ISSN: 0363-6399 the whole document	7,8,12, 21,25,26
A	HERFERT M: "SECURITY-ENHANCED MAILING LISTS" IEEE NETWORK: THE MAGAZINE OF COMPUTER COMMUNICATIONS, vol. 11, no. 3, 1 May 1997 (1997-05-01), pages 30-33, XP000689787 ISSN: 0890-8044 the whole document	15,28
A	WO 97 00471 A (DOGON GIL ;KRAMER SHLOMO (IL); SHWED GIL (IL); ZUK NIR (IL); BEN R) 3 January 1997 (1997-01-03) abstract page 4, line 1 -page 7, line 18 figures 1,3,16	29
A	GB 2 323 757 A (IBM) 30 September 1998 (1998-09-30) abstract page 2, line 35 -page 4, line 21 page 9, line 39 -page 10, line 4 figures 4,9	29
A	SMITH R E: "A SECURE EMAIL GATEWAY (BUILDING AN RCAS EXTERNAL INTERFACE)" PROCEEDINGS. ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE,1994, XP002912413 the whole document	29

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

rnational Application No
PCT/SE 99/02021

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9747106 A	11-12-1997	US 5862220 A	19-01-1999
		AU 3223897 A	05-01-1998
		EP 0900491 A	10-03-1999
WO 9613113 A	02-05-1996	US 5864683 A	26-01-1999
		AU 3888595 A	15-05-1996
		EP 0787397 A	06-08-1997
WO 9700471 A	03-01-1997	US 5606668 A	25-02-1997
		AU 6135696 A	15-01-1997
		CA 2197548 A	03-01-1997
		EP 0807347 A	19-11-1997
		JP 10504168 T	14-04-1998
		NO 970611 A	15-04-1997
		US 5835726 A	10-11-1998
		CA 2138058 A	16-06-1995
		EP 0658837 A	21-06-1995
		JP 8044642 A	16-02-1996
GB 2323757 A	30-09-1998	JP 10285216 A	23-10-1998